TAD:ELM
F. #2017R01297

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF A WHITE SAMSUNG GALAXY S7 EDGE CELLULAR TELEPHONE WITH SERIAL NUMBER SM-G935T AND IMEI NUMBER 357751075565314, SEIZED ON JULY 9, 2017	APPLICATION FOR SEARCH WARRANT Case No. 18M095

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR WARRANT TO SEARCH AND SEIZE

I, TENITRIS N. MCINNIS, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 1(c) of the Federal Rules of Criminal Procedure, Rule 41 of the Federal Rules of Criminal Procedure, the inherent authority of the district court to issue warrants under Article III of the United States Constitution, and the Fourth Amendment to the United States Constitution,[1] for a search

[1] In United States v. Villegas, 899 F.2d 1324, 1334 (2d Cir. 1990), the Court of Appeals for the Second Circuit stated that "Rule 41 does not define the extent of the court's power to issue a search warrant," and "[o]bviously, the Fourth Amendment long antedated the Federal Rules of Criminal Procedure, which were first adopted in 1944." The Second Circuit further recognized that: "[g]iven the Fourth Amendment's warrant requirements, and assuming no statutory prohibitions, the courts must be deemed to have inherent power to issue a warrant when the requirements of that Amendment are met." Id. (internal citations omitted).

warrant authorizing the examination of an electronic device currently in law enforcement custody, more particularly described in Attachment A, and the extraction from that device of electronically stored information described in Attachment B.

2. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), and have been for approximately three years. Prior to becoming a Special Agent with the ATF, I was a police officer with the Tallahassee Police Department for over seven years. During the past ten years, I have personally participated in numerous investigations and arrests, the debriefing of cooperating witnesses and informants, and the execution of numerous search warrants, including search warrants for electronic devices. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information contained in this affidavit includes information that I obtained from other law enforcement agents and officers, and from law enforcement and public records databases. The statements described in this affidavit are set forth in sum, substance, and in part.

IDENTIFICATION OF THE PROPERTY TO BE SEARCHED

4. This affidavit is submitted in support of an application for a warrant to search a full forensic image (the "Image") of A WHITE SAMSUNG GALAXY S7 EDGE CELLULAR TELEPHONE WITH SERIAL NUMBER SM-G935T AND IMEI NUMBER 357751075565314, SEIZED ON JULY 9, 2017 (the "Device"). The Device and the Image

are currently being transported, via FedEx, from Washington, D.C., to the United States Attorney's Office for the Eastern District of New York ("USAO").

5. On January 23, 2018, the Honorable Viktor V. Pohorelsky issued a search warrant (the "January Warrant") permitting a full forensic examination of the Device for the purpose of identifying and seizing the following limited categories of electronically stored information: a list of all calls placed from the Device and all calls received from the Device and all text messages received by the Device, including any pre-populated information concerning the identity of the persons with whom the Device was communicating, but excluding the content of any such calls or text messages (collectively, "call and text logs"), for the period May 1, 2017 to July 10, 2017. Copies of the affidavit in support of the January Warrant and the January Warrant are attached hereto as Exhibit A.

6. On or about January 24, 2018, an ATF agent attempted to forensically examine the Device to obtain the call and text logs, but could not do so because the phone was locked. The same ATF agent then sent the Device to the Department of Justice's Cybercrime Laboratory in Washington, D.C. (the "Cybercrime Lab"), to seek assistance in obtaining a forensic image of the Device. After multiple unsuccessful attempts to unlock the Device, obtain a forensic image of it, and seize the call and text logs, on January 31, 2018, the Cybercrime Lab obtained the Image. The Image is password protected. Neither I nor any member of the ATF or the USAO has viewed or accessed the Image. Consistent with the January Warrant, on February 1, 2018, I received and reviewed files from the Cybercrime Lab containing the call and text logs.

PROBABLE CAUSE

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that ANTHONY WIGGINS and others known and unknown have committed and are committing violations of federal criminal law, including unlawful possession of a firearm by a prohibited person, in violation of Title 18, United States Code, Section 922, and access device fraud, in violation of Title 18, United States Code, Section 1029(a), and conspiracy to commit access device fraud, in violation of Title 18, United States Code, Section 1029(b)(2) (the "Subject Offenses"). There is also probable cause to search the Image described in Attachment A for evidence, instrumentalities, contraband and/or fruits of these crimes further described in Attachment B.

I. THE MAY 29, 2017 SEARCH OF THE DEFENDANT'S HOME

8. On or about May 29, 2017, Denise Grant was arrested by the New York City Police Department ("NYPD") at her home at 1423 Saint Marks Avenue, Apartment 2, in Brooklyn, New York (the "Saint Marks Apartment") following a domestic dispute with her sister, Jayda Grant. At the time of her arrest, NYPD officers discovered a single R-P .380 auto bullet in the pocket of Denise Grant's pants during a search incident to her arrest.

9. During a post-arrest debriefing, Denise Grant denied ownership of the bullet, and stated that she was wearing her boyfriend Anthony's pants. By running a series of database checks, NYPD officers determined that Denise Grant's boyfriend was ANTHONY WIGGINS.

10. On or about May 29, 2017, NYPD officers went to the Saint Marks Apartment to further investigate the origin of the bullet recovered from the pocket of Denise Grant's

pants. When the officers arrived, Jayda Grant was the only person at home. Jayda Grant consented in writing to a search of the Saint Marks Apartment. NYPD officers also obtained verbal consent to search the Saint Marks Apartment from Denise Grant and Jayda Grant's mother, who also lived in the Saint Marks Apartment, over the telephone.

11. During the course of the search, NYPD officers discovered a shoebox located in plain view inside a bedroom. The shoebox contained eleven fraudulent credit and debit cards and drivers licenses, including two fraudulent credit cards in Denise Grant's name and one card in Eqwanna Crawford's name. The driver's licenses contained photos of two individuals, and each driver's license contained a different name and address for the two individuals. Denise Grant and Eqwanna Crawford have close relationships with ANTHONY WIGGINS. Denise Grant is WIGGINS' long-term girlfriend, and was listed as the emergency contact on WIGGINS' United States Marshals Service processing paperwork. Eqwanna Crawford and WIGGINS have two children together. Both Denise Grant and Eqwanna Crawford offered to sign as suretors on WIGGINS' bond in connection with his July 9, 2017 arrest.

12. Both Denise Grant and Eqwanna Crawford have maintained regular contact via email and telephone with WIGGINS since his incarceration at Rikers and at the Metropolitan Detention Center ("MDC") in connection with his July 9, 2017 arrest, described below. Since his arrest, WIGGINS has instructed Denise Grant, via the MDC's monitored email system, to update his social media accounts – including his Facebook and Instagram accounts.

13. The shoebox also contained an empty, Hi-point brand .380-caliber magazine, and a 9-millimeter bullet. In addition, the shoebox contained Kings County court documents and a New York City Department of Corrections and Community Supervision identification card, all in the name of ANTHONY WIGGINS. The NYPD officers also discovered two forged temporary license plates under the bed.

14. Based on WIGGINS' demonstrated contact with both Denise Grant and Eqwanna Crawford from May 2017 to the present via phone and email, in addition to the presence of both Denise Grant's and Eqwanna Crawford's names on the fraudulent credit cards found in the shoebox in the Saint Marks Apartment on May 29, 2017, there is probable cause to believe that the Device and the Image contain evidence of violations of 18 U.S.C. § 1029(a)(1) and § 1029(b)(2), including text messages, social media communications and photographs between WIGGINS and Denise Grant and WIGGINS and Eqwanna Crawford.

15. Indeed, text logs recovered from the Device show that on June 9, 2017, the Device sent an outgoing MMS[2] to (631) 620-9803, the same telephone number Denise Grant provided to the NYPD when she was arrested on May 29, 2017 (the "Grant Phone"). On the same Date, the Device received a MMS from the Grant Phone. The Device did not contain MMS, SMS or call logs pre-dating June 9, 2017, which suggests that WIGGINS obtained the Device on or about June 9, 2017. Based on my training and experience with smartphones, there is a high likelihood that the Device contains photos, social media messages and other

---

[2] MMS stands for "multimedia messaging service," a means of sending messages that include multimedia content such as images, video, or voice recordings, from a mobile phone over a cellular network.

content that pre-dates June 9, 2017. That is because many people transfer the contents of their previous phones to their new phones. Indeed, stores that sell smartphones will often transfer the content of previous phones to new phones, using cloud-based services, when a new smartphone is purchased. The call and text logs obtained from the Device showed frequent communication between WIGGINS and the Grant Phone between June 9, 2017 and July 9, 2017. Given the closeness in time to Grant's arrest and the consent search of the Saint Mark's Apartment, both of which occurred on May 29, 2017, and the repeated MMS communications between the Device and the Grant Phone from June 9, 2017 to July 9, 2017, there is probable cause to believe that the Image will contain evidence concerning the defendant's ownership of the bullet, empty magazine and fraudulent access devices contained found in the shoebox.

II. THE JULY 6, 2017 BURGLARY OF BASIL PIZZA AND WINE BAR

16. Basil Pizza and Wine Bar ("Basil") is a restaurant located at 270 Kingston Avenue, in Brooklyn, New York. On or about July 6, 2017, at approximately 1:30 a.m., three individuals wearing bandanas and hooded sweatshirts broke the restaurant's lock and burglarized Basil. The owner of Basil reported to the NYPD that numerous Apple iPads, a combination safe, and approximately $8,000 were stolen during the burglary.

17. The Device contained multiple incoming and outgoing call logs in the hours before the Basil burglary, as well as multiple incoming and outgoing text messages. The call logs reveal that at 10:44 p.m. on July 5, 2017, less than three hours before the Basil burglary, the Device received an incoming call from "Blu," from the number (718) 496-1093. The call lasted approximately two minutes and eighteen seconds. Based on an NYPD complaint

report, number appears to belong to Antique Jenkins, an associate of WIGGINS, who has five prior felony arrests and two prior felony convictions, including a March 14, 2016 arrest for Intimidating a Victim or Witness in the Third Degree, a Class E Felony, and Tampering With a Witness in the Third Degree, a Class E Felony. On or about October 10, 2017, Atique Jenkins was convicted upon a plea of guilty to Tampering with a Witness in the Fourth Degree to Induce Him To Not Appear/Testify at Proceeding, a Class A misdemeanor, and was sentenced to a one-year order of protection. On August 11, 2011, Atique Jenkins was convicted, pursuant to a plea of guilty, for Criminal Possession of a Weapon in the Fourth Degree. At 11:49 p.m. on July 5, 2017, less than two hours before the Basil burglary, the Device received an incoming call from "Gee Money" from the telephone number (347) 447-8254, a prepaid phone. Based on my training and experience, individuals who are involved in criminal activity often use prepaid phones to avoid detection. At 11:49 p.m. and 11:56 p.m., the Device sent an outgoing SMS messages to the Grant Phone. At 3:45 a.m., approximately two hours after the Basil robbery, the Device sent two outgoing SMS messages to the Grant Phone.

III. THE DEFENDANT'S JULY 9, 2017 ARREST

18. At approximately 4:30 a.m. on July 9, 2017, three plainclothes NYPD police officers assigned to the 77th Precinct were driving at a slow rate of speed in an unmarked car west on Prospect Place in Brooklyn, New York, towards Nostrand Avenue, with the windows down. Prospect Place was well lit by streetlights and security lights posted on apartment buildings along the block. Officer #1 was sitting in the rear, passenger-side seat, Officer #2 was sitting in the front, passenger-side seat, and Officer #3 was driving. As the

officers drove along Prospect Place, they observed an individual, later identified as ANTHONY WIGGINS, standing on the sidewalk, facing against the flow of traffic on Prospect Place. The defendant was wearing a tight black t-shirt and dark, close-fitting pants.

19. Officer #1 observed the butt of a firearm sticking out of the defendant's waistband. Officer #1 exited the vehicle and made eye contact with ANTHONY WIGGINS. Officer #1's shield was visible, and he identified himself as a police officer.

20. Officer #1 commanded ANTHONY WIGGINS not to move. ANTHONY WIGGINS immediately and without hesitation ran directly into the apartment building located at 805 Prospect Place (the "Prospect Place Building"), and up the stairs. Officer #1 and Officer #2 pursued the defendant on foot into the Prospect Place Building and up the staircase. Officer #2 was familiar with the Prospect Place Building based on his experience in the 77th Precinct, and he knew it to be frequented by members of the Bergen Family gang, who used at least one apartment within the Prospect Place Building to further and conceal evidence of criminal activity, including credit card fraud, illegal weapons and drug distribution.

21. As ANTHONY WIGGINS approached the third floor landing at a run, with Officer #1 in close pursuit, Officer #1 observed WIGGINS attempt to pick up a black backpack (the "Backpack"), which was on the staircase near the third floor landing. WIGGINS could not maintain his grasp on the Backpack while running up the steps, and he dropped the Backpack near the third floor landing.

22. Officer #1 and Officer #2 followed ANTHONY WIGGINS up the stairs to the roof of the apartment building. Officer #1, who was using a flashlight, observed the firearm

drop from ANTHONY WIGGINS' waistband onto the roof of the Prospect Place Building. ANTHONY WIGGINS then attempted to escape down a fire escape, but he then turned around and went back up the fire escape to the roof. After a brief struggle, Officer #1 and Officer # 2 placed ANTHONY WIGGINS under arrest.

23. Officer #1 recovered a loaded, .357-caliber Colt revolver with defaced serial numbers (the "Firearm") from the Prospect Place Building's roof, where ANTHONY WIGGINS had dropped it. The officers also seized and vouchered a portable, Masterlock-brand combination safe, which they found on the roof of the Prospect Place Building (the "Safe"). The back panel of the Safe had been pried off at the time it was recovered, and there was nothing inside.

24. Additionally, NYPD officers seized the Backpack from the stairwell of the Prospect Place Building. The Backpack contained five Apple iPads. The iPads were charged and unlocked at the time of the seizure, and, when activated, all showed menus for Basil, which was located approximately seven blocks from the Prospect Place Building. As described above, Basil had been burglarized approximately three days earlier, and the owner of Basil reported that multiple iPads had been stolen from the restaurant.

25. NYPD officers transported ANTHONY WIGGINS from the Prospect Place Building to the 77th Precinct. At the 77th Precinct, NYPD officers seized the Device from ANTHONY WIGGINS and vouchered it as evidence. At the time of its seizure, the Device was damaged, and its screen was cracked. The Device remained in the custody of the NYPD until on or about January 9, 2018, when ATF agents took possession of the Device. Neither

the NYPD nor the ATF conducted a forensic search of the Device at any point between its seizure on July 9, 2017 and January 23, 2018.

26. Call and text logs from the Device show an incoming voice call on July 8, 2017 at 9:31 p.m. from (212) 477-3063 (the "3063" number), which lasted approximately one minute and thirty-two seconds. The 3063 number belongs to Javon Pope, who has numerous prior arrests for narcotics distribution.

27. During the time immediately leading up to WIGGINS' arrest for possessing a firearm after having been convicted of a felony, the Device received a number of calls and messages. On July 9, 2017, the Device received an incoming call at approximately 2:41 a.m. that lasted approximately twenty-one seconds. On July 9, 2017, between 2:54 a.m. and 4:15 a.m., the Device received thirteen missed calls from various numbers, including Denise Grant, Atique Jenkins, and the prepaid phone associated with "Gee Money." On July 9, 2017, between 2:14 a.m. and 3:31 a.m., the Device received fourteen SMS messages from various individuals, including Atique Jenkins, "Gee Money," "MellowNew" and an unidentified number that appears as "1111" in the Device's text logs.

28. NYPD officers also recovered a New York State identification card from ANTHONY WIGGINS at the time of his arrest. The identification card listed ANTHONY WIGGINS' address as the Saint Marks Apartment, the location where the bullet and empty magazine were recovered. ANTHONY WIGGINS possessed $500 in cash at the time of his arrest. WIGGINS possessed one $100 bill and twenty $20 bills. Based on my training and experience, the possession of $500 in cash and a loaded revolver in close proximity to a known drug trafficking location, is consistent with drug trafficking activity.

29. NYPD officers took a series of photos of WIGGINS after he was arrested. The photos show WIGGINS' face from the front and side, and a small portion of the black t-shirt WIGGINS was wearing on July 9, 2017. The photos do not show the full t-shirt WIGGINS was wearing that day, nor do they show the tight-fitting pants that the firearm was tucked into. WIGGINS was initially arrested on state charges, and he was detained at Rikers Island. I am aware that when a pre-trial detainee is first detained at Rikers, the New York City Department of Correction ("DOC") seizes the detainee's clothing, and the detainee's clothing is then stored. When he was indicted on the instant federal charges, WIGGINS was transferred to the custody of the United States Marshals Service, in the detention clothing Rikers provided to WIGGINS. In advance of trial, the defense identified the clothing WIGGINS was wearing on the date of his arrest as potential trial exhibits. From this, I infer that someone retrieved WIGGINS' clothing from Rikers and has retained the clothing since that time. However, I do not know what, if anything, has been done to WIGGINS' clothing after it was retrieved from Rikers, nor do I know if WIGGINS is the same weight he was when he was arrested. Photos of WIGGINS on the Device that depict the clothing he was wearing on July 9, 2017 are relevant to the charged crime, because the characteristics of his clothing will corroborate the officers' testimony about how they could see the firearm.

30. I have reviewed criminal history records indicating that before July 9, 2017, ANTHONY WIGGINS had previously been convicted of a crime punishable by a term of imprisonment exceeding one year. WIGGINS was convicted of robbery in the third degree, in violation of New York Penal Law § 160.05, a crime punishable by a term of imprisonment

of more than one year, for which the Kings County Supreme Court sentenced the defendant to one to three years' imprisonment on March 2, 2009.

31. On August 4, 2017, a grand jury sitting in the Eastern District of New York returned a two-count indictment charging ANTHONY WIGGINS with being a felon unlawfully in possession of a firearm, in violation of 18 U.S.C. § 922(g)(1), and with possession of a firearm with an obliterated serial number, in violation of 18 U.S.C. § 922(k). (See 17-CR-419 (NGG).)

II. THE DEVICE AND IMAGE

32. Based on my training and experience and the call and text logs on the Device, I believe that a review of the information stored on Image, including text messages sent or received by ANTHONY WIGGINS, voice memos made by ANTHONY WIGGINS, voice messages received by ANTHONY WIGGINS, social media posts and messages sent or received by ANTHONY WIGGINS, and photos taken, sent or received by ANTHONY WIGGINS will identify the individuals with whom WIGGINS was communicating prior to the discovery of the fraudulent credit cards at the Saint Marks Apartment on May 29, 2017, their means and methods of communication, as well from whom ANTHONY WIGGINS obtained the fraudulent credit cards, how he obtained those credit cards, and what he intended to do with those credit cards. The Image may also contain photographs of WIGGINS surrounding the May 29, 2017 discovery of the magazine and bullet in the shoebox in the Saint Marks Apartment. Such photographs may include ANTHONY WIGGINS in the room in the Saint Marks Apartment where the shoebox and fraudulent identification was found; photographs of ANTHONY WIGGINS wearing the sweatpants that

Denise Grant stated belonged to her boyfriend; and communications between ANTHONY WIGGINS and Denise Grant about the NYPD search of the Saint Marks Apartment. Information contained on the Device may include with whom WIGGINS was communicating prior to the discovery of the ammunition at the Saint Marks Apartment on May 29, 2017, their means and methods of communication, as well from whom ANTHONY WIGGINS obtained the ammunition, and for what purpose he obtained the ammunition.

33. Additionally, based on my training and experience and my review of the call and text logs on the Device, I believe that a review of the information stored on the Image, including messages sent or received by ANTHONY WIGGINS, social media posts and messages sent or received by ANTHONY WIGGINS, and photos sent or received by ANTHONY WIGGINS, will reveal photographs of WIGGINS with the firearm and ammunition he possessed on July 9, 2017, photographs of WIGGINS in the clothing he was wearing on July 9, 2017, and messages that explain why WIGGINS was in the vicinity of the Prospect Place Building on July 9, 2017, including his familiarity with the Prospect Place Building, and his association with gang members and affiliates who live in or use the Prospect Place Building as a stash house.

34. The Device and the Image are being transported from Washington, D.C. to the USAO. As described above, the NYPD seized the Device from ANTHONY WIGGINS when he was arrested on July 9, 2017. The ATF obtained the Device from the NYPD in January 2018. Based on my training and experience, I know that Image was obtained in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the NYPD. On

January 22, 2018, the ATF and the U.S. Attorney's Office for the Eastern District of New York requested WIGGINS' consent to search the Device, through WIGGINS' counsel. Counsel refused to consent to a search of the Device.

TECHNICAL TERMS

35. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones.

b. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. If the telephone number that is communicating with the wireless telephone is stored as a "contact" in the wireless telephone's "address book," as described below, the call log will access that information, and, where the available, provide related "contact" information. Based on my training and experience, I know that it may be necessary to perform a forensic extraction of all data saved on the Device in order to generate a report of the Device's call log, including related "contact" information. To the extent that this warrant seeks content, such content is limited to the "contact" information that is automatically populated in the Device's call log.

c. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers as specified "contacts" in an electronic "address book;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

d. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

e. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage

media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

f. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

g. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless

communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

36. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a web browser, email client, Internet messaging device, telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

37. Based on my knowledge, training and experience, I know that those who are engaged in conspiracies often communicate with co-conspirators to plan and execute crimes by means of wireless telephone (including by means of text messages, electronic mail and social media messages), and record the contact information of criminal associates in the "contacts" section of such telephones. Those who commit such offenses may retain evidence of their participation in such offenses on wireless telephones through call records, text messages, WhatsApp messages, Facebook messages, Instagram messages, emails or photos. That data (including communications and photographs) may also constitute evidence of their association with criminal organizations, conspiracies and/or enterprise. Moreover, information stored on such telephone, including photographs, emails and text messages, can be used to help identify the users of such telephones.

38. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

39. There is probable cause to believe that things that were once stored on the Device are on the Image, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for

years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

40. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Image:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file, or messages that have been sent or received by the user of a cellular telephone but have been subsequently deleted). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device to communicate with coconspirators regarding an agreement to unlawfully transfer firearms or to distribute controlled substances, including marijuana and cocaine, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is

also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

41. *Nature of examination.* Based on the foregoing, and consistent with Rule 1(c), 41(e)(2)(B), the inherent authority of the district court to issue warrants under Article III of the United States Constitution, and the Fourth Amendment to the United States Constitution, the warrant I am applying for would permit the examination of the Image consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Image to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

42. I submit that this affidavit supports probable cause for a search warrant authorizing law enforcement to search the Image described in Attachment A to conduct a forensic examination for the purpose of identifying the electronically stored information described in Attachment B.

Respectfully submitted,

TENITRIS N. MCINNIS
Special Agent
Bureau of Alcohol, Tobacco, Firearms and Explosives

Subscribed and sworn to before me
on February 2, 2018:

THE HONORABLE NICHOLAS G. GARAUFIS
UNITED STATES DISTRICT JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Description of the Property to Be Searched

THE FORENSIC IMAGE OF A WHITE SAMSUNG GALAXY S7 EDGE CELLULAR TELEPHONE WITH SERIAL NUMBER SM-G935T AND IMEI NUMBER 357751075565314 ("DEVICE"), SEIZED ON JULY 9, 2017, THAT IS EN ROUTE FROM WASHINGTON, D.C., TO THE EASTERN DISTRICT OF NEW YORK (hereinafter, the "IMAGE")

This warrant authorizes the forensic examination of the IMAGE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Description of the Things to Be Seized

1. All records and information on the Image described in Attachment A that relate to violations of 18 U.S.C. §§ 922, 1029(a) and 1029(b)(2) involving ANTHONY WIGGINS and any co-conspirators (the "Subject Individuals"), since May 1, 2017, including:

a. any information related to the possession of firearms or ammunition by the Subject Individuals;

b. any information related to WIGGINS' familiarity with 805 Prospect Place, Brooklyn, New York, including any GPS data showing that WIGGINS had at 805 Prospect Place prior to July 9, 2017;

c. lists of or contact information for individuals dealing in firearms or ammunition, and related identifying information;

d. types, amounts, and prices of firearms and ammunition purchased as well as dates, places, and amounts of specific transactions;

e. any information related to sources of firearms (including names, addresses, phone numbers, or any other identifying information);

f. any information related to sources of stolen personal identifying or financial information (including names, addresses, phone numbers, or any other identifying information);

g. any information related to the purchase or sale of access devices, or access device-making equipment;

h. any information related to transactions involving the use of a fraudulent access device by any of the Subject Individuals;

i. any information recording the Subject Individuals' locations from May 1, 2017, to the present;

j. all bank records, checks, credit card bills, account information, and other financial records;

k. photographs, video, text messages, instant messages and all other electronic communications, saved audio files, web browsing history and other records reflecting communications to and from the Subject Individuals, and photos, video, text messages, instant messages and all other electronic communications showing ANTHONY WIGGINS' clothing, including the fit of his clothing, on July 9, 2017;

l. records of or information about the DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. statements and other information regarding firearms trafficking activity, identity theft, fraud and violent crimes;

n. evidence indicating the user of the DEVICE's state of mind as it relates to the crimes under investigation.

2. Evidence of user attribution showing who used or owned the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs,

phonebooks, saved usernames and passwords, self-identifying information and photographs, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.